September 15, 2005

Testimony of

Dave Kepler

Corporate Vice President of Shared Services and
Chief Information Officer
The Dow Chemical Company

Before the

The Committee on Science of the U.S. House of Representatives

"Cybersecurity: U.S. Vulnerability and Preparedness."

Thank you Chairman Boehlert and Ranking Member Gordon for allowing me to share my thoughts on this important topic.

Mr. Chairman, before I begin, our thoughts and prayers go out to the millions of Americans, including many of our 7,000 employees on the gulf coast who have lost so much from hurricane Katrina.

Our number one priority is the safety and well-being of our employees and the communities impacted by this disaster. We are committed to safely returning our facilities to full operation and contributing to the recovery efforts. The importance of information infrastructure for communications and emergency response in a national crisis has never been more apparent.

I'm Dave Kepler, Corporate Vice President of Shared Services and Chief Information Officer of The Dow Chemical Company. Dow is the world's largest chemical and plastics producer with annual sales of over $40 billion serving customers in markets such as: food, transportation, health and medicine, personal and home care, and building and construction.

I am also here as the Chairman of the Executive Board of the Chemical Sector Cybersecurity Program. This effort was established in 2002 to coordinate the sector's activity and to align with the U.S. government's National Strategy to Secure Cyberspace. The program's mission is to understand the risks we face as a sector and coordinate and prioritize our efforts to reduce those risks. Leadership for this program is provided by the chemical industry's leading CIOs, and leverages expertise from existing organizations: chemical trade associations, the Chemical Industry Data Exchange, and the Chemical Sector Information Sharing and Analysis Center.

The five strategic elements of the program are:

- Broad support and participation throughout the sector
- Engagement with government to ensure effective measures to secure cyberspace
- Identification and reduction of infrastructure vulnerabilities to guard against cyber attacks and speed recovery from incidents
- Establishment of management practices and guidance to support overall sector cyber security

- Ongoing coordination with technology providers, government and academia to accelerate development of improved, cost-effective solutions

The program produced comprehensive cyber security guidance which was built into the Responsible Care Security Code in 2004. Implementation of the Responsible Care Security Code is mandatory for all members of the American Chemistry Council and has also been adopted by the Synthetic Organic Chemical Manufacturers Association.

Our sector continues to work closely with the Department of Homeland Security, standards bodies such as the National Institute of Standards and Technology (NIST) and industry organizations such as Instrumentation Systems and Automation (ISA) to share the latest best practices and to develop new standards to defend against cyber attacks.

Today, I would like to discuss the role of information technology in our sector, describe the cyber security threats we face and highlight what is being done to address these threats. I will also suggest areas where the government can help.

Let me begin by outlining the importance of our sector to our nation's economic well-being and security-- enabling 25% of our nation's GDP. With $109 billion dollars in exports, the chemical industry is the largest exporter in the US economy. We employ one million Americans and are one of the largest private industry investors in research and development. Our industry makes modern life possible, from plastics to pharmaceuticals, from cars to clothing. Our products help keep the water we drink safe, increase productivity of agriculture, and enable medical innovations that prevent and treat disease. Our industry is also essential to homeland defense and the war on terror -- making products that go into bullet-resistant vests, night vision goggles and stealth aircraft.

Our industry's safety culture and history of cooperative voluntary initiatives, partnerships with local, state and federal government agencies, and strong support for research and development, position us well to address new security challenges. For example, the industry joined forces to develop the American Chemistry Council's Responsible Care Security Code -- building upon long-standing industry safety and emergency response programs.

All aspects of security are integrated into the Security Code including physical plant security, transportation security, as well as cyber security. Implementation of the Responsible Care Security Code is mandatory for all American Chemistry Council members leading to over $2 billion in investments to improve security and preparedness across our industry.

Cyber security has been on our radar screen long before the tragic events of 9/11. At Dow, for example, we have had policies and practices in place for securing our information assets for many years. These cover the use of the Internet, integration of systems, and automation of manufacturing control. The emergence of a significant terrorist threat with the events of 9/11 added urgency and focus to our efforts. It was this event that prompted the establishment of the Chemical Sector Cyber Security program.

It's in our national interest to have a competitive chemical industry, and information technology is key in maintaining that competitiveness. At Dow, information technology is fully integrated into all aspects of our business -- research and development, manufacturing, accounting, logistics and sales to name just a few. We also use information technology to interact with government agencies and to report our regulatory compliance. Advanced technology is also being leveraged to secure our facilities and the distribution of our products. We rely on automation and integration of our processes to drive productivity, quality, and safety.

At Dow, approximately 15% of our orders are via the Internet, and nearly all of our customers use the Internet to learn about our products, track orders, and get technical support. The Internet is also a valuable communications tool -- essential to public safety and emergency response. For example, in the aftermath of Katrina when all phone service was disrupted, Dow was able to use Internet based phones to communicate with our facilities in the region.

In 2004, chemical company executives conducted an industry-level vulnerability assessment to determine the potential impact of cyber security threats. We concluded that, unlike an attack on other critical infrastructures, a cyber security breach would not cause cascading impact across the chemical industry.

We believe the higher concern for our industry is the potential of a combined physical and cyber attack or the criminal use of illegally obtained information.

There are three specific areas of concern for the chemical industry:

1. Using information on shipments, product inventory, or sites to construct a physical attack. That's why Dow has set in place policies, practices and technologies to protect the linkage of critical plant systems with corporate networks.

2. Using false identity to acquire chemicals for improper use. Our company counters this threat by pre-identifying and verifying our customers before electronic orders.

3. Gaining inappropriate access to systems to cause isolated disruptions. At Dow, operating practices and authentication technology is continuously being upgraded to restrict what people can do based on roles and clearances.

For obvious reasons, I cannot get into all we do to protect ourselves, but here are some additional steps that Dow has taken to combat these threats.

Addressing people, processes and technology, we have:

- Developed a company-wide cyber security management plan that includes incident management and business continuity.

- Completed a comprehensive cyber security risk analysis based on the ISO information security standard, ISO/IEC 17799.

- Used the U.S. government Sandia National Labs methodology for assessing vulnerability of our sites and manufacturing facilities – including a review of physical, process, and cyber vulnerabilities.

We continue to test and upgrade our plans in all areas of security.

Although much has been done within the chemical sector, we cannot address cyber security threats alone. Security of the nation's telecommunications and Internet infrastructure is beyond any one sector's control. Protecting the nation's critical communication and information infrastructure from a significant attack, whether physical, cyber, or combined, is of the utmost importance.

So, what role should the government play? While there are many issues impacting secure computing today such as random hacking and the email virus of the day, the Department of Homeland Security must contend with the real threat of attacks by people, organizations or nations -- intent on causing significant disruption to our economy and way of life. Targeted attacks that could have a major economic or social impact must be the priority as well as protecting our communications capability in the event of a national emergency.

Department of Homeland Security resources and research and development efforts should be dedicated to addressing these 'big picture' threats to benefit all sectors and improve our national security. Threat monitoring and modeling, better methods for authenticating identity, and information protection should be research priorities. Efforts should include understanding how to prevent attacks, what resources and tools are needed to defend against attacks, and what it would take to reconstitute our information technology infrastructure in the event of a catastrophic failure.

We are encouraged by the Department's work with the public and private sectors to reduce vulnerabilities and minimize the severity of cyber attacks. But, more needs to be done around the sharing and protection of relevant information across all critical sectors and government. Finally, government crisis management and disaster recovery plans must include industry participation. As witnessed in the aftermath of Katrina -- coordinated emergency response, ongoing monitoring, and managed recovery efforts with government and industry are critical.

We believe continued and expanded cooperation between our critical sector, the Department of Homeland Security and other government agencies as well as information technology providers is vital to reduce vulnerabilities and enhance preparedness.

Any efforts to improve cyber security must:

- Start and end with the commitment to be a risk-based, outcome-focused program. DHS must focus on the real threat of criminal attacks by people, organizations or nations.

- Recognize that cyber security is an integral part of overall security, and build upon the work to date of the chemical sector security programs such as the Responsible Care Security Code and the Chemical Sector Cybersecurity Program.

- Recognize the high degree of integration of the chemical sector with other critical infrastructure sectors, as well as the importance of our industry to our homeland defense and economic security.

In closing, we are committed to ensuring the security of our company and to taking a leadership role in improving overall security across our industry. Information sharing and continued cooperation between our sector and the Department of Homeland Security is critical. Above all else, efforts must be focused on those threats of greatest impact and concern to our national security, while addressing the unique needs of each sector.

Thank you and I'd be happy to answer any questions.

Biography
David E. Kepler

D. E. (Dave) Kepler is corporate vice president of Shared Services and chief information officer (CIO) of The Dow Chemical Company. In this capacity, Kepler has global responsibility for Customer Service, Information Systems, Purchasing, Six Sigma, Supply Chain and Work Process Improvement. He is also a member of the Office of the Chief Executive (OCE).

Kepler joined Dow in 1975 in the Western Division Computer and Process Systems group. After progressive Commercial and Information Systems roles throughout the United States, Canada and the Pacific, he was named director of Chemicals and Plastics Information Systems in 1993. In 1995, Kepler assumed additional responsibility as director of Global Information Systems Applications. He was appointed vice president and CIO in February 1998, and in 2000, assumed the role of corporate vice president of eBusiness. In 2002, Kepler undertook commercial responsibility for the Advanced Electronic Materials business and further expanded his role the following year, adding responsibility for Global Purchasing and Supply Chain. Kepler assumed his most recent role in January 2004.

Kepler serves on the Board of Directors of the U.S. Chamber of Commerce. He is a member of the American Chemical Society and the American Institute of Chemical Engineers. In addition, he leads the Executive Committee of the Chemical Sector Cybersecurity Program. Locally, Kepler serves on the Board of Directors for the Midland Community Cancer Services and Alden B. Dow Museum of Science and Art. He was the 2004 United Way of Midland County Campaign Chair.

Kepler received a bachelor's degree in chemical engineering from the University of California at Berkeley.